

# Notice of Allowability

Application No.

10/015,377

Examiner

Longbit Chai

Applicant(s)

BROCK ET AL.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to interview on 5/8/2006.
2. ☒ The allowed claim(s) is/are 31 and 32.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

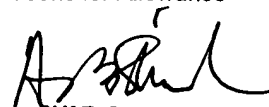
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 5/8/2006.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

  
AYAZ SHEIKH

SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

## **DETAILED ACTION**

### ***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Arthur J. Samodovitz (Reg. No. 31,297) on 5/8/2006.

This application has been amended as follows:

#### **IN THE CLAIMS**

Cancel claims 1 – 30.

Replace claims 31 and 32 as follows.

#### **Claim 31:**

A method of detecting intrusions, said method comprising the steps of:  
storing a plurality of intrusion signatures;  
automatically detecting a multiplicity of system events having respective signatures;

comparing each of the multiplicity of system event signatures to said plurality of intrusion signatures, one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures; and

storing said one system event signature in association with said plurality of intrusion signatures not corresponding to an intrusion;

recording a number of times that said each of said intrusion signatures matches a respective one of said system event signatures;

recording a number of times that said one system event has occurred;

subsequently ordering the stored plurality of intrusion signatures and said one system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order; and

subsequently comparing a signature of a subsequent system event with said signatures in said order until finding a match between said subsequent system event signature and one of said signatures in said order.

**Claim 32:**

A system for detecting intrusions, said system comprising:

a table storing a plurality of intrusion signatures;

Art Unit: 2131

means for detecting a multiplicity of system events having respective signatures;

means for comparing *each of* the multiplicity of system event signatures to said plurality of intrusion signatures, one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures;

means for storing said one system event signature in association with said plurality of intrusion signatures not corresponding to an intrusion;

means for recording a number of times that each of said intrusion signatures matches a respective one of said system event signatures;

means for recording a number of times that said one system event has occurred;

means for subsequently ordering the stored plurality of intrusion signatures and said one system event signature based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order; and

means for subsequently comparing a signature of a subsequent system event with said signatures in said order until finding a match between said subsequent system event signature and one of said signatures in said order.

***Allowable Subject Matter***

1. Claims 31 and 32 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 31 and 32.

The prior art Vaidya fails to teach or suggest means for subsequently ordering the stored plurality of intrusion signatures and said one system event signature not corresponding to an intrusion based on the respective number of times that have been recorded for said plurality of intrusion signatures and said one system event signature, such that the signature for which the most number of times has been recorded is first in the order. Besides, the prior art fail to teach compare each of the multiplicity of system event signatures to said plurality of intrusion signatures, one of said system event signatures not matching any of said intrusion signatures and not corresponding to an intrusion, and other of said system event signatures matching respective ones of said intrusion signatures; and storing said one system event signature in association with said plurality of intrusion signatures not corresponding to an intrusion.


Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

LBC